# SLOVENSKI STANDARD
# oSIST prEN 13608-1:2006

**01-februar-2006**

---

**Zdravstvena informatika – Varnost komuniciranja v zdravstvenem varstvu – 1. del: Koncepti in izrazje**

Health informatics - Security for healthcare communication - Part 1: Concepts and terminology

Medizinische Informatik - Sicherheit für die Kommunikation im Gesundheitswesen - Teil 1: Konzepte und Terminologie



Informatique de Santé - Sécurité des communications dans le domaine de la santé - Partie 1: Concepts et Terminologie



**Ta slovenski standard je istoveten z:** **prEN 13608-1**

---

**ICS:**

| | | |
|---|---|---|
| 01.040.35 | Informacijska tehnologija. Pisarniški stroji (Slovarji) | Information technology. Office machines (Vocabularies) |
| 35.240.80 | Uporabniške rešitve IT v zdravstveni tehniki | IT applications in health care technology |

**oSIST prEN 13608-1:2006** **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# DRAFT
# prEN 13608-1

November 2005

ICS

Will supersede ENV 13608-1:2000

English Version

# Health informatics - Security for healthcare communication - Part 1: Concepts and terminology

Informatique de Santé - Sécurité des communications dans le domaine de la santé - Partie 1: Concepts et Terminologie

Gesundheitsinformatik - Sicherheit für Kommunikation im Gesundheitswesen - Teil 1: Konzepte und Terminologie

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 251.

If this draft becomes a European Standard, CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the Management Centre has the same status as the official versions.



CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.



Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

**Warning** : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

**Management Centre: rue de Stassart, 36 B-1050 Brussels**



Ref. No. prEN 13608-1:2005: E

# Contents

Page

# Foreword

This document (prEN 13608-1:2005) has been prepared by Technical Committee CEN/TC 251 “Health informatics”, the secretariat of which is held by SIS.

This document is currently submitted to the CEN Enquiry.

This document will supersede ENV 13608-1:2000.

EN 13608 consists of the following parts, under the general title *Health informatics — Security for Healthcare Communication (SEC-COM):*

— *Part 1: Concepts and Terminology*

— *Part 2: Secure Data Objects*

— *Part 3: Secure Data Channels*

This standard is designed to meet the demands of the Technical Report CEN/TC251/N98-110 *Health Informatics — Framework for security protection of health care communication*.



This standard is drafted using the conventions of the ISO/IEC Directive Part 3.



All annexes are informative.

# Introduction

This multipart standard (prEN 13608) on Security for healthcare communication can be applied to a wide range of communication protocols and information system applications relevant to healthcare, though they are neither complete nor exhaustive in that respect.

Part 1 – Concepts and Terminology – reflects a user-requirements driven approach and a methodology for the analysis of the relation between 1) user needs and 2) a technological solution. At the core of this methodology is the Policy Bridging Model (PBM) constituting the policy bridging process. The essential concepts of the PBM are defined in chapter 5, and the more detailed process defined in chapter 6. The methodology begins with a standardised way of expressing user needs, continues through technology-oriented successive refinements of the corresponding required security solutions and ends with a standard-oriented map of the corresponding recommended security solutions. Such a method can be utilised in many ways, out of which the two most important usages are:

1) as a general, stand-alone tool for breaking down user needs into technological solutions, through a process/journey of close collaboration between users and security experts, and

2) through using this common (normative) method in the standardization process, establishing a link between a defined set of user needs and a technological standard. Such a link carries an *a priori* assurance on the effectiveness of the technological standards in terms of complying with the user needs. Such an *a priori* assurance will be of special value for the user that do not want to exercise the method in detail on his/her own, but merely want to *benefit from an established, and in that sense normative, link* between a set of user needs that he/she can recognise, and the existence of an implementation standard.



The PBM and its methodology is organised by means of a matrix, and the path through this matrix from the user needs to a technological solution may be viewed as the standard for the specification of a Communication Protection Profile (CPP), according to CEN/TC251/N98-110.

prEN 13608-2 [1)] and prEN 13608-3 [1)] are examples of clause 2 mentioned above. prEN13608 as a whole is designed for further extensions (prEN 13608-x) based on the same scheme.

It is of paramount importance for the understanding of this methodology of prEN 13608-1, to recognise that it comprises a journey from user needs to detailed technological specifications, and that several distinct perspectives and contexts are undertaken along this journey. In particular, it is important to recognise that commonly used (already existing, e.g. ISO) standards are comparable to only a subset of the total number of contexts defined by the method. E.g. it has been necessary to introduce the concept of *auditability* for the *user need context*, because the more commonly used notion of *accountability* is perceived to have a more *limited* and *technical constitution*.

Different user views will imply different patterns of use of the matrix. For standardization purposes (to constitute a valid CPP), the matrix must be filled out in detail (however only in those parts that are applicable for a selection of user needs). This process provides some level of *assurance* that the actual technological solution is an *effective* representation of the user needs defined in the actual CPP. The method itself does not specify in detail how each specific cell of the matrix shall appear. Annexes B-J provide examples that may be viewed as guidelines, of which Annexes B and C has a special role because of their correspondence with the already existing prEN 13608-2 and prEN 13608-3.

1) To be published.

Thus, this Part 1 offers a set of different *views* or *journeys* through the successive refinement from user need to technological solution. The security journey on the most detailed level is a *combination* of :

1) top-down approach, by allowing for a systematic translation from a common policy expression, down to technological choices and options;

2) bottom-up approach, by being focused on utilisation of existing, commercial technologies.

Hence, the CPP concept must not be understood as a purely deductive (one-way) development *from* user needs *to* technological solution, but merely as a (standardised) statement that gives evidential indication that a specific technological standard, is an *effective and reasonable fulfilment* of a specific set of user needs.

Hence, the normative function of Part 1 can be summarised as:

1) standardising the way of expressing a communication security policy;

2) standardising the steps of successive refinements down to the technology level, in order to provide a minimum level of assurance [2)].

The benefit for a end-user is that he can look for a CPP that matches his demand for:

a) a matching set of user needs;

b) a technological context (e.g. EDI);

and successively identifies:



c) a named implementation standard (e.g. Annexes B and C that corresponds with prEN 13608-2 and prEN 13608-3, respectively).



In the latter case, the standardisation process offers the user a degree of assurance that a product meeting the implementation standard effectively meets the user needs described in the Part 1 annex. Alternatively, if such a standard is not found, he/she can use the method in cooperation with security experts, to constitute a basis from which can be identified the needs and their effective solutions.

Figure 1 below depicts how the matrix is used methodologically to constitute relations between user needs, technological contexts and implementation standards.

2) The actual level of assurance achieved is not comparable to what can be achieved through a security evaluation process, cfr Annex K.

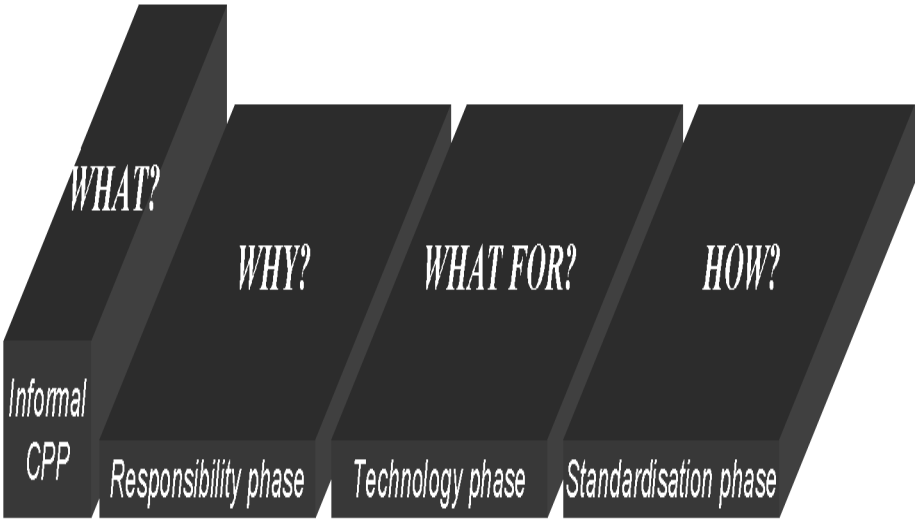


**Figure 1 — The Security Policy Bridging phases**



Parts 2 and 3 are examples of implementation standards that have a CPP counterpart, as they both are described in terms of Part 1 requirements (in Annex B and C). Both are based on rather simplistic technological solutions, however with a wide installed base in healthcare and with a large potential for future use. Both of them are based on commercial technologies with an existing product portfolio.



The method prescribed by Part 1 is however open in the sense that other pairs of CPP-standard can be developed in the future – e.g. based on other technological concepts such as middleware, WWW-based systems etc. These will successively be named pr EN 13608-4 and so on, and will be complemented by new annexes in prEN 13608-1.

In order to provide external coherence:

— Annex A provides some examples and illustrations of the usage of this SEC-COM part 1 in terms of general security concepts, with a refined proposal for the auditability property;

— Annexes D to J indicate what a selection of *other* security standards actually can currently offer in regard of the SEC-COM method;

— In Annex K, the relation between the assurance gained through the method, and the assurance gained in a security evaluation based on Common Criteria, is discussed.

**Possible future extensions of scope for 13608**

Communicating parties (sender and receiver) using a common prEN 13608-X standard will implicitly be using the same communication security police. The CPP approach defined by prEN 13608-1 can however in the future be given an even wider implication. The CPP approach may also facilitate a more dynamic *security policy bridging* between sender and receiver, that is, a policy bridging that may be negotiated before actual communication between the parties. Such a negotiation will require a "standardised" description of the embodiment of the site (communication) security policy. In the simplest case, the prEN 13608-1 (chapter 5) way of expressing a (communication) security policy may be a (informal) basis for deciding whether to communicate or not. Moreover, the systematic refinement of a (communication) security policy down to a

more technical level constitutes the basis for a more automatic and precise decision process (semiformal). Such a (possible) process may thus consist of three different steps, based on the PBM (as illustrated in Figure 2 below):

a) the first step is the *Terminology Linking* one, ensuring that any communicating entity will be able to use and understand a *common* security policy language,

b) the second step is the *Policy Matching* one, ensuring that any communicating entity will be able to compare and match his own communication security policy with any peer entity's communication security policy,

c) the third step is the *Policy Negotiation* one, ensuring that any communicating entity will be able to adapt his own communication security policy in order to be able to adopt a common communication security policy (common in that it is shared by his communication peer entities).

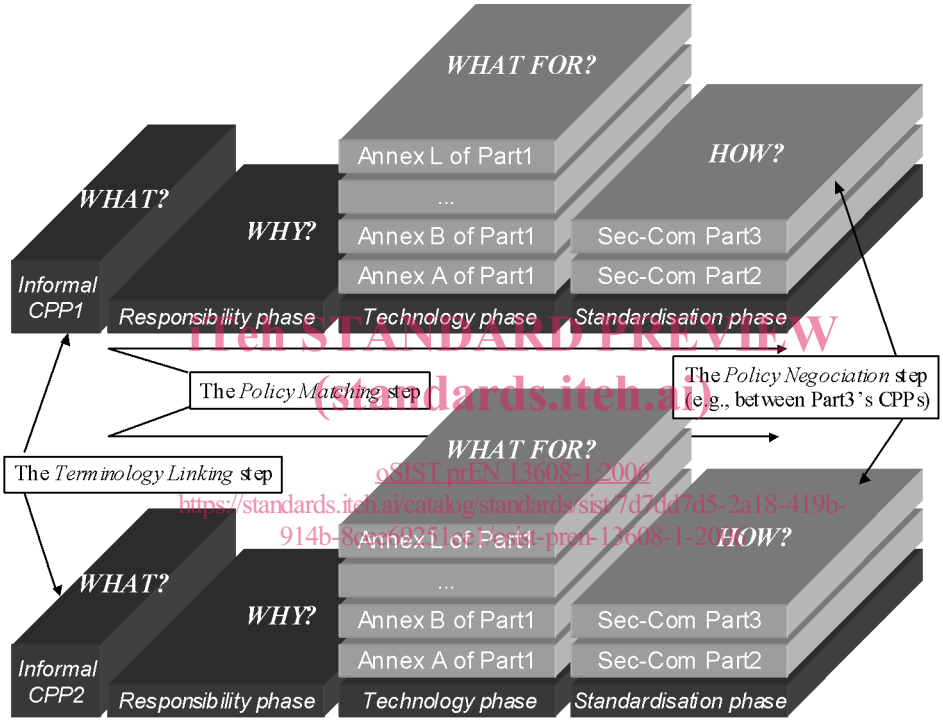




**Figure 2 — The Security Policy Bridging steps**

## 1 Scope

This European standard specifies a methodology for defining, expressing and selecting a communication protection profile (CPP) specification, and thus provides:

1) a standard way of expressing healthcare user security needs in relation to communication;

2) a standard method of successive refinement of policy statements, hereby helping to identify standardised security implementation specification that can be utilised to meet these security needs.

Security aspects contained within the communication protection profile include integrity, confidentiality, and availability, and also auditability.

This methodology shall thus serve the purpose of being a tool for:

A. the end-user in collaboration with security experts, while seeking effective solutions for relevant and powerful healthcare communication security needs;

B. the standardization process in which trustworthy links between 1) actual selections of such user needs and 2) technological standards, are established.

## 2 Normative references



The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.



ISO/IEC 2382-8, *Information technology — Vocabulary — Part 8: Security*.

ISO 7498-2, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*.

ISO 9594-8, *Information technology — Open Systems Interconnection — The Directory: Authentication framework*.

ISO 10181-1, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview*.

ISO 8824-1:1995, *Information Technology — Abstract syntax notation one (ASN.1) — Part 1: Specification of basic notation*.

ISO 9735-4, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number : 4) — Part 4: Syntax and service report message for batch EDI (message type CONTRL)*.

ISO 9735-5, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number : 4) — Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)*.

ISO 9735-6, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number : 4) — Part 6: Secure authentication and acknowledgement message (message type AUTACK)*.

ISO 9735-7, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (syntax version number 4) — Part 7: Security rules for batch EDI (confidentiality).*

ITU/CCITT X.435, Message Handling Systems: Electronic Data Interchange Messaging System (X.435 Recommendation).

ITU/CCITT F.435, Message Handling Services: Electronic Data Interchange Messaging Services (F.435 Recommendation).

PKCS#7, Cryptographic Message Syntax Version 1.5, RFC 2315.

Common Criteria V2, Common Criteria for Information Technology Security Evaluation V2.0 – July 1998.

ECMA TR/46, European Computer Manufacturers Association — Security in Open Systems: A Security Framework.

ITSEC, Information Technology Security Evaluation Criteria – June 1991.

Federal Criteria, US Federal Criteria for Information Technology Security – December 1992.

TCSEC, US Department of Defence – Trusted Computer System Evaluation Criteria – Dec. 1985.

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

**3.1**
**abstract security mechanisms**
security mechanism described in a generalised fashion, without specific choices made for algorithms



**3.2**
**access control**
a means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

[ISO/IEC 2382-8]]

**3.3**
**accountability**
the property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO 7498-2]

**3.4**
**asymmetric cryptographic algorithm**
an algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ

[ISO 10181-1]

**3.5**
**auditability**
the property that ensures that any action of any security subject on any security object may be examined in order to establish the real operational responsibilities

NOTE In the SEC-COM series the *auditability* property, considered as encompassing several sub-properties contributing to the transfer of responsibility in the message transport system and also proving authorship, is not defined as synonymous with the classical *accountability* property, but as encompassing it as indicated by its refinement in the informative Annex A.

**3.6**
**authentication**
process of reliably identifying security subjects by securely associating an identifier and its authenticator. See also data origin authentication and peer entity authentication

[ISO 7498-2]

**3.7**
**authenticator**
piece of information that confirms a claimed identity by transforming a successful identification into a successful authentication

**3.8**
**authorization**
the granting of rights, which includes the granting of access based on access rights

[ISO 7498-2]

**3.9**
**availability**
property of being accessible and useable upon demand by an authorised entity

[ISO 7498-2]

**3.10**
**certificate distribution**
act of publishing certificates and transferring certificates to security subjects



**3.11**
**certificate generation**
act of creating certificates



**3.12**
**certificate management**
procedures relating to certificates: certificate generation, certificate distribution, certificate archiving

**3.13**
**certificate revocation**
act of removing any reliable link between a certificate and its related owner (or security subject owner), because the certificate is not trusted any more whereas it is unexpired

**3.14**
**certificate holder**
an entity that is named as the subject of a valid certificate

**3.15**
**certificate user**
an entity that needs to know, with certainty, the public key of another entity

[ISO 9594-8]

**3.16**
**certificate verification**
verifying that a certificate is authentic

**3.17**
**certification**
use of digital signature to make transferable statement about beliefs of identity, or statements about delegation of authority

**3.18**
**certification authority**
an authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys

[ISO 9594-8]

**3.19**
**ciphertext**
data produced through the use of encipherment. The semantic content of the resulting data is not available

[ISO 7498-2]

**3.20**
**ciphersuite**
an encoding for the set of bulk data cipher, message digest function, digital signature algorithm and key exchange algorithm used within the negotiation phase of TLS

**3.21**
**communication destination**
**destination**
a security subject involved in a communication in the general sense that it is the address to which the sensitive information is sent by other security subject

**3.22**
**communication originator**
**originator**
a security subject involved in a communication in the generic sense that it is the origin from where the sensitive information is sent to other security subjects



**3.23**
**communication transporter**
**transporter**
a security subject involved in a communication which is contractually responsible for transporting sensitive information from communicating senders to communicating receivers

**3.24**
**communication protection profile**
**CPP**
a statement of systematic translation form communication security needs to technological concepts

**3.25**
**communicating sender**
**sender**
a security subject involved in a communication which is legally responsible for sending sensitive information to other security subjects

NOTE *Sender* is a special case for *Originator*, in the restricted sense of active communication entity.

**3.26**
**communicating receiver**
**receiver**
a security subject involved in a communication which is legally responsible for receiving sensitive information from other security subjects

NOTE *Receiver* is a special case of *Destination* in the restricted sense of an active communication entity.

**3.27**
**communicating carrier**
**carrier**
a security subject involved in a communication which is legally responsible for transporting sensitive information from communicating senders to communicating receivers

NOTE *Receiver* is a special case of *Transporter* in the restricted sense of an active communication entity.

**3.28**
**communication third party**
**repository**
a security subject optionally involved in a communication which is legally responsible for notarisation of information to provide an independent attestation of a security property where a conflict of interests potentially exists between the communicating parties

NOTE A *Repository*, in the sense of an active communication entity for which legally notarisation responsibility has been recognised by all the communicating parties, is a case of third party for the communication context.

**3.29**
**communication security**
security of security objects communicated between security subjects

**3.30**
**confidentiality**
the property that information is not made available or disclosed to unauthorised individuals, entities, or processes



[ISO 7498-2]

**3.31**
**cryptography**
the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use



[ISO 7498-2]

**3.32**
**cryptographic algorithm**
**cipher**
an algorithm used to transform data to hide its information content which is used in the process of encryption (see 3.37)

**3.33**
**data integrity**
The property that data has not been altered or destroyed in an unauthorised manner

[ISO 7498-2]

**3.34**
**data origin authentication**
the corroboration that the source of data received is as claimed

[ISO 7498-2]

**3.35**
**decryption**
**decipherment**
process of making encrypted data reappear in its original unencrypted form. The reversal of a corresponding reversible encipherment